FortiOS - Release Notes

Version 6.2.11

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 22, 2022
FortiOS 6.2.11 Release Notes
01-6211-792573-20220622

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-06-22	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 6.2.11 build 1303.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.2.11 supports the following models.

FortiGate	FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30E-MG, FG-40F, FG-40F-3G4G, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-400E-BP, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-5001D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-40F, FWF-40F-3G4G, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE
FortiGate Rugged	FGR-30D, FGR-35D, FGR-60F, FGR-60F-3G4G, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special branch supported models

The following models are released on a special branch of FortiOS 6.2.11. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1303.

FG-80D	is released on build 5207.
FG-200F	is released on build 7241.
FG-201F	is released on build 7241.

Special notices

New Fortinet cloud services

FortiOS 6.2.0 introduced several new cloud-based services listed below. The new services require updates to FortiCare and Fortinet's FortiCloud single sign-on (SSO) service.

- Overlay Controller VPN
- FortiGuard Cloud-Assist SD-WAN Interface Bandwidth Monitoring
- FortiManager Cloud
- FortiAnalyzer Cloud

FortiGuard Security Rating Service

Not all FortiGate models can support running the FortiGuard Security Rating Service as a Fabric "root" device. The following FortiGate platforms can run the FortiGuard Security Rating Service when added to an existing Fortinet Security Fabric managed by a supported FortiGate model:

- FGR-30D
- FGR-35D
- FGT-30E
- FGT-30E-MI
- FGT-30E-MN
- FGT-50E
- FGT-51E

- FGT-52E
- FWF-30E
- FWF-30E-MI
- FWF-30E-MN
- FWF-50E
- FWF-50E-2R
- FWF-51E

Using FortiManager as a FortiGuard server

If you use FortiManager as a FortiGuard server, and you configure the FortiGate to use a secure connection to FortiManager, you must use HTTPS with port 8888. HTTPS with port 53 is not supported.

FortiGate hardware limitation

FortiOS 5.4.0 reported an issue with the FG-92D model in the *Special Notices* > *FG-92D High Availability in Interface Mode* section of the release notes. Those issues, which were related to the use of port 1 through 14, include:

- PPPoE failing, HA failing to form.
- IPv6 packets being dropped.
- FortiSwitch devices failing to be discovered.
- Spanning tree loops may result depending on the network topology.

FG-92D does not support STP. These issues have been improved in FortiOS 5.4.1, but with some side effects with the introduction of a new command, which is enabled by default:

```
config global
   set hw-switch-ether-filter <enable | disable>
```

When the command is enabled:

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed.
- BPDUs are dropped and therefore no STP loop results.
- PPPoE packets are dropped.
- IPv6 packets are dropped.
- FortiSwitch devices are not discovered.
- HA may fail to form depending the network topology.

When the command is disabled:

- All packet types are allowed, but depending on the network topology, an STP loop may result.

CAPWAP traffic offloading

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip. The following models are affected:

- FG-900D
- FG-1000D
- FG-2000E
- FG-2500E

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

NP4lite platforms

FortiOS 6.2 and later does not support NP4lite platforms.

Tags option removed from GUI

The Tags option is removed from the GUI. This includes the following:

- The *System* > *Tags* page is removed.
- The *Tags* section is removed from all pages that had a *Tags* section.
- The *Tags* column is removed from all column selections.

L2TP over IPsec on certain mobile devices

Bug ID	Description
459996	Samsung Galaxy Tab A 8 and Android 9.0 crash after L2TP over IPsec is connected.

PCI passthrough ports

Bug ID	Description
605103	PCI passthrough ports order might be changed after upgrading. This does not affect VMXNET3 and SR-IOV ports because SR-IOV ports are in MAC order by default.

SSL traffic over TLS 1.0 will not be checked and will be bypassed by default

FortiOS 6.2.6 and 6.4.3 ended support for TLS 1.0 when `strong-crypto` is enabled under `system global`. With this change, SSL traffic over TLS 1.0 will not be checked so it will be bypassed by default.

To examine and/or block TLS 1.0 traffic, an administrator can either:

- Disable `strong-crypto` under `config system global`. This applies to FortiOS 6.2.6 and 6.4.3, or later versions.
- Under `config firewall ssl-ssh-profile`:
  - in FortiOS 6.2.6 and later, set `unsupported-ssl` to `block`.
  - in FortiOS 6.4.3 and later, set `unsupported-ssl-negotiation` to `block`.

FortiGate 80D release

The FortiGate 80D released in 6.2.9 and later includes the removal of the LTE modem feature using the USB port on that model.

FortiGate 100D transceiver information removed

FortiOS 6.2.10 has removed the display of transceiver information on the *Network* > *Interfaces* page and the `get system interface transceiver` command.

New features or enhancements

Bug ID	Description
613155	Add two-factor authentication support to VPN IKEv2 for remote RADIUS and LDAP users.

745135	Provide three sizes of internet service databases and an option to choose between full, standard, and mini databases. The FortiGate 30 and 50 series can only configure the mini size.
	`config system global`
	`    set internet-service-database {mini | standard | full}`
	`end`

Upgrade Information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

FortiGate 30E and 50E flash card space optimization

On FortiGate 30 and 50 series models, the flash and /data partition may run out of space, that can cause errors after upgrade. The following models are affected:

- FortiGate 30E and 50E series
- FortiWifi 30E and 50E series
- FortiGate Rugged 30D and 35D

To resolve this issue:

1. Install the GEOIP V2 Database on FortiGate 30 and 50 models, which uses less space on the flash card than the GEOIP v3 Database installed on other models.
2. Provide a smaller Internet Service Database (ISDB) specifically for the FortiGate 30 and 50 models, and force these models to use this smaller ISDB.
3. Move the IPS Database to the /data2 partition to reduce space on the /data partition.

To upgrade successfully:

The output of disk spaced used in the partitions requires the use of a debug build and internal command. They are shown as reference only, based on a FortiGate 51E.

1. Since the initial state of the /data partition on the flash card is close to 100%, manually delete the GEOIP Database to avoid upgrade failure or loss of configuration files when upgrading the firmware:

```
# diagnose geoip delete-geoip-db
This operation will delete the Geoip Database and reboot the system!
```

```
Only super admin has the permission with the command.
Do you want to continue? (y/n)y
Admin:admin
Password: ********
File /etc/geoip_db.gz deleted successfully.
After reboot, please update to the latest GeoDB version from FortiGuard server, with
command 'execute update-geo-ip'.
If connection to FortiGuard is not available, please upgrade the FOS firmware after
reboot.
#
The system is going down NOW !!
```

The FortiGate will automatically restart to free up space. Do not run `execute update-geo-ip` after the system reboots and before you perform the upgrade.

Note the partition size before and after the GEOIP Database is deleted.

Before	97% /data 93% /data2
After	82% /data 93% /data2

2. Upgrade the FortiGate to the new firmware. Once completed, the GEOIP V2 Database is installed. Verify the installation:

```
# diagnose autoupdate versions | grep -A 2 Geography
IP Geography DB
---------
Version: 2.00114
```

3. The new firmware will force the FortiGate 30 and 50 models to use the smaller ISDB. Update the ISDB to the smaller database using FortiGuard:

```
# execute update-now
```

Once updated, additional space under the /data2 partition is available. Note the partition size before and after the smaller ISDB is installed.

Before	84% /data 95% /data2
After	85% /data 76% /data2

4. Manually restart the FortiGate to allow the IPS Database to move to the /data2 partition.

The space used in the /data and /data2 partitions are now reduced compared to before the upgrade.

FortiClient Endpoint Telemetry license

Starting with FortiOS 6.2.0, the FortiClient Endpoint Telemetry license is deprecated. The FortiClient Compliance profile under the Security Profiles menu has been removed as has the Enforce FortiClient Compliance Check option under each interface configuration page. Endpoints running FortiClient 6.2.0 now register only with FortiClient EMS 6.2.0 and compliance is accomplished through the use of Compliance Verification Rules configured on FortiClient EMS 6.2.0 and enforced through the use of firewall policies. As a result, there are two upgrade scenarios:

- Customers using only a FortiGate device in FortiOS 6.0 to enforce compliance must install FortiClient EMS 6.2.0 and purchase a FortiClient Security Fabric Agent License for their FortiClient EMS installation.
- Customers using both a FortiGate device in FortiOS 6.0 and FortiClient EMS running 6.0 for compliance enforcement, must upgrade the FortiGate device to FortiOS 6.2.0, FortiClient to 6.2.0, and FortiClient EMS to 6.2.0.

The FortiClient 6.2.0 for MS Windows standard installer and zip package containing FortiClient.msi and language transforms and the FortiClient 6.2.0 for macOS standard installer are included with FortiClient EMS 6.2.0.

Fortinet Security Fabric upgrade

FortiOS 6.2.11 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.2.5
- FortiClient EMS 6.2.3 and later
- FortiClient 6.2.3 and later
- FortiAP 5.4.4 and later
- FortiSwitch 3.6.11 and later

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiADC
13. FortiDDOS
14. FortiWLC

If the Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.2.11. When the Security Fabric is enabled in FortiOS 6.2.11, all FortiGate devices must be running FortiOS 6.2.11.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.2.11 uses the `ssl-min-proto-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.2.11 and later, the default `ssl-min-proto-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)
- FortiSandbox (`config system fortisandbox`)
- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)
- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Amazon AWS enhanced networking compatibility issue

With this enhancement, there is a compatibility issue with 5.6.2 and older AWS VM versions. After downgrading a 6.2.11 image to a 5.6.2 or older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 6.2.11 to 5.6.2 or older versions, running the enhanced NIC driver is not allowed. The following AWS instances are affected:

C5	Inf1	P3	T3a
C5d	m4.16xlarge	R4	u-6tb1.metal
C5n	M5	R5	u-9tb1.metal
F1	M5a	R5a	u-12tb1.metal
G3	M5ad	R5ad	u-18tb1.metal
G4	M5d	R5d	u-24tb1.metal
H1	M5dn	R5dn	X1
I3	M5n	R5n	X1e
I3en	P2	T3	z1d

A workaround is to stop the instance, change the type to a non-ENA driver NIC type, and continue with downgrading.

FortiLink access-profile setting

The new FortiLink `local-access` profile controls access to the physical interface of a FortiSwitch that is managed by FortiGate.

After upgrading FortiGate to 6.2.11, the interface `allowaccess` configuration on all managed FortiSwitches are overwritten by the default FortiGate `local-access` profile. You must manually add your protocols to the `local-access` profile after upgrading to 6.2.11.

To configure `local-access` profile:

```
config switch-controller security-policy local-access
    edit [Policy Name]
        set mgmt-allowaccess https ping ssh
        set internal-allowaccess https ping ssh
    next
end
```

To apply `local-access` profile to managed FortiSwitch:

```
config switch-controller managed-switch
    edit [FortiSwitch Serial Number]
        set switch-profile [Policy Name]
        set access-profile [Policy Name]
    next
end
```

FortiGate VM with V-license

This version allows FortiGate VM with V-License to enable `split-vdom`.

To enable `split-vdom`:

```
config system global
   set vdom-mode [no-vdom | split vdom]
end
```

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiGuard update-server-location setting

The FortiGuard `update-server-location` default setting is different between hardware platforms and VMs. On hardware platforms, the default is `any`. On VMs, the default is `usa`.

On VMs, after upgrading from 5.6.3 or earlier to 5.6.4 or later (including 6.0.0 or later), `update-server-location` is set to `usa`.

If necessary, set `update-server-location` to use the nearest or low-latency FDS servers.

To set FortiGuard `update-server-location`:

```
config system fortiguard
   set update-server-location [usa|any]
end
```

FortiView widgets

FortiView widgets have been rewritten in 6.2.0. FortiView widgets created in previous versions are deleted in the upgrade.

Product integration and support

The following table lists FortiOS 6.2.11 product integration and support information:

Web Browsers	• Microsoft Edge • Mozilla Firefox version 93 • Google Chrome version 95 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge • Mozilla Firefox version 93 • Google Chrome version 95 • Microsoft Internet Explorer version 11 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 14. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Fortinet Security Fabric upgrade on page 14. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient: • **Microsoft Windows** • **Mac OS X** • **Linux**	• 6.2.0 See important compatibility information in FortiClient Endpoint Telemetry license on page 14 and Fortinet Security Fabric upgrade on page 14. FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later. If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 5.6.0 and later are supported.
FortiClient iOS	• 6.2.0 and later
FortiClient Android and FortiClient VPN Android	• 6.2.0 and later
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later
FortiAP-U	• 5.4.5 and later
FortiAP-W2	• 5.6.0 and later

FortiSwitch OS (FortiLink support)	• 3.6.9 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 and later
Fortinet Single Sign-On (FSSO)	• 5.0 build 0306 and later (needed for FSSO agent support OU in group filters) • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 (32-bit and 64-bit) • Windows Server 2008 R2 64-bit • Windows Server 2008 Core • Novell eDirectory 8.8
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 4.0 version.
AV Engine	• 6.00165
IPS Engine	• 5.00267
Virtualization Environments	
Citrix	• Hypervisor Express 8.1, build 2019-12-04
Linux KVM	• Ubuntu 18.04.3 LTS • QEMU emulator version 4.4.4 (Debian 1:4.0+dfsg-0ubuntu9.4) • libvirtd (libvirt) 4.0.0
Microsoft	• Hyper-V Server 2019
Open Source	• XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04 / 18.04 (32-bit & 64-bit)	2336. Download from the Fortinet Developer Network: https://fndn.fortinet.net.

Other operating systems may function correctly, but are not supported by Fortinet.

SSL VPN standalone client no longer supports the following operating systems:

- Microsoft Windows 7 (32-bit & 64-bit)
- Microsoft Windows 8 / 8.1 (32-bit & 64-bit)
- Microsoft Windows 10 (64-bit)
- Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 93 Google Chrome version 95
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 93 Google Chrome version 95
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 93 Google Chrome version 95
macOS Monterey 12.0	Apple Safari version 15 Mozilla Firefox version 93 Google Chrome version 95
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

Supported Microsoft Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection 11	✓	✓
Kaspersky Antivirus 2009	✓	
McAfee Security Center 8.1	✓	✓
Trend Micro Internet Security Pro	✓	✓
F-Secure Internet Security 2009	✓	✓

Supported Microsoft Windows 7 32-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✓	✓
AVG Internet Security 2011		
F-Secure Internet Security 2011	✓	✓
Kaspersky Internet Security 2011	✓	✓
McAfee Internet Security 2011	✓	✓
Norton 360™ Version 4.0	✓	✓
Norton™ Internet Security 2011	✓	✓
Panda Internet Security 2011	✓	✓
Sophos Security Suite	✓	✓
Trend Micro Titanium Internet Security	✓	✓
ZoneAlarm Security Suite	✓	✓
Symantec Endpoint Protection Small Business Edition 12.0	✓	✓

Resolved issues

The following issues have been fixed in version 6.2.11. For inquires about a particular bug, please contact Customer Service & Support.

Explicit Proxy

Bug ID	Description
765761	Firewall with forward proxy and UTM enabled is sending TLS probe with forward proxy IP instead of real server IP.

Firewall

Bug ID	Description
629529	Local-in policy session will not update after policy changes.
738584	Firewall is using the wrong NAT IP address to send out traffic after removing the VIP and its associated policy.
770668	The packet dropped counter is not incremented for `per-ip-shaper` with `max-concurrent-session` as the only criterion and offload disabled on the firewall policy.

GUI

Bug ID	Description
746953	On the *Network* > *Interfaces* page, users cannot modify the TFTP server setting. A warning with the message *This option may not function correctly. It is already configured using the CLI attribute: tftp-server.* appears beside the *DHCP Options* entry.
749451	On the *Network* > *SD-WAN* page, the volume sent/received displayed in the charts does not match the values provided from the REST API when the RX and TX values of `diagnose sys sdwan intf-sla-log` exceed 2^{32}-1.

HA

Bug ID	Description
627968	Local-in policy with `ha-mgmt-intf-only` enabled is not installed properly.
640327	Duplicate logs are created by both primary and secondary devices for IPsec VPN.
779512	If the interface name is a number, an error occurs when that number is used as an `hbdev` priority.

Intrusion Prevention

Bug ID	Description
682071	IPS signatures not working with VIP in proxy mode.
698247	Flow mode web filter `ovrd` crashes and socket leaks in IPS daemon.
715360	Each time an AV database update occurs (scheduled or manually triggered), the IPS engine restarts on the SLBC secondary blade.
755859	The IPS sessions count is higher than system sessions, which causes the FortiGate to enter conserve mode.
775696	Each time an AV database update occurs (scheduled or manual), the IPS engine restarts on the SLBC secondary blade. This stops UTM analysis for sessions affected by that blade.

IPsec VPN

Bug ID	Description
715671	Traffic is failing on dialup VPN IKEv2 with EAP authentication.
726326, 745331	IPsec server with NP offloading drops packets with an invalid SPI during rekey.

Log & Report

Bug ID	Description
764478	Logs are missing on FortiGate Cloud from the FortiGate.

Proxy

Bug ID	Description
603874	WAD may encounter memory corruption issue if the resources allocated by FTS are not cleaned up properly.
692444	WAD memory leak is caused by missing a close event. The WAD receives a close event from TCP when the SSL port is blocked by the up application layer. If the SSL port input buffer does not have any data, then the close event will get ignored even if the application layer turns off blocking and the SSL port will leak.
693441	WAD crashes at `wad_client_cert_req_act_get` when SSL layer configuration is cleaned up after policy matching.
729237	WAD crash occurs that is related to virtual server traffic.

Security Fabric

Bug ID	Description
686420	Dynamic address resolution is lost when SDN connector sends `sync.callback` command to the FortiGate.
690812	FortiGate firewall dynamic address resolution lost when SDN connector updates its cache.

SSL VPN

Bug ID	Description
677057	SSL VPN firewall policy creation via CLI does not require setting user identity.
737894	If there are no users or groups in an SSL VPN policy, the SSL VPN daemon may crash when an FQDN is a destination address in the firewall policy.
771162	Unable to access SSL VPN bookmark in web mode.

Switch Controller

Bug ID	Description
740661	FortiGate loses FortiSwitch management access due to excessive configuration pushes.

System

Bug ID	Description
627054	HTTPSD signal 6 crash in cases of long application lists that are greater or equal to the maximum size of 16.
642958	FG-80E terminates the firewall session abruptly when the end-users download large files.
651626	A session clash is caused by the same NAT port. It happens when many sessions are created at the same time and they get the same NAT port due to the wrong port seed value.
662239	FGR-60F-3G4G hardware switch span does not work.
671116	Lack of null pointer check in NP6XLite driver may lead to kernel panic. Affected models: FG-40F, FG-60F, and FG-101F.
681322	TCP 8008 permitted by authd, even though the service in the policy does not include that port.
682681	DSL line takes a long time to synchronize.
703219, 708446	Kernel panic on FG-101F due to lack of null pointer check on NP6XLite driver.
712321	Multiple ports flapping when a single interface is manually brought up. Affected platforms: FG-3810D and FG-3815D.
749613	Unable to save configuration changes, and get `failed: No space left on device` error on FG-61E, FG-81E, and FG-101E.
749835	Traffic logs reports ICMP destination as unreachable for received traffic
750171	Legitimate traffic is unable to go through with NP6 `synproxy` enabled.
751523	When changing mode from DHCP to static, the existing DHCP IP is kept so no CLI command is generated and sent to FortiManager.
754951	Static ARP entry was removed while using DHCP relay.
763185	High CPU usage on platforms with low free memory upon IPS engine initialization.
765452	On FG-100F, no event is raised for PSU failure and the diagnostic command is not available.
778474	dhcpd is not processing discover messages if they contain a 0 length option, such as 80 (rapid commit). The warning, `length 0 overflows input buffer`, is displayed.

Upgrade

Bug ID	Description
685705	After upgrading to 6.2.6, get errors `No such file or directory` and `No space left on device` on FWF-50 and FWF-51E.

User & Device

Bug ID	Description
604906	FortiOS does not prompt for token when using RADIUS and two-factor authentication to connect to IPsec IKEv2.
757883	FortiGate blocks expired root CA, even if the cross-signed intermediate CA of the root CA is valid.

VM

Bug ID	Description
759300	gcpd has signal 11 crash at `gcpd_mime_part_end`.

Web Filter

Bug ID	Description
801792	IPS daemon has socket FD leaks.
806920	Incomplete TCP handshake with NP offloading enabled on policies with wireless interfaces.

WiFi Controller

Bug ID	Description
720497	MAC authentication bypass is not working for some clients.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
689909	FortiOS 6.2.11 is no longer vulnerable to the following CVE Reference: • CVE-2022-22306
695018	FortiOS 6.2.11 is no longer vulnerable to the following CVE Reference:

Bug ID	CVE references
	• CVE-2022-22306
707951	FortiOS 6.2.11 is no longer vulnerable to the following CVE Reference: • CVE-2021-41032
763982	FortiOS 6.2.11 is no longer vulnerable to the following CVE Reference: • CVE-2021-43081
764221	FortiOS 6.2.11 is no longer vulnerable to the following CVE Reference: • CVE-2021-43206

Known issues

The following issues have been identified in version 6.2.11. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

DNS Filter

Bug ID	Description
582374	License shows expiry date of `0000-00-00`.

Explicit Proxy

Bug ID	Description
540091	Cannot access explicit FTP proxy via VIP.

Firewall

Bug ID	Description
654356	In NGFW policy mode, sessions are not re-validated when security policies are changed. **Workaround**: clear the session after policy change.

FortiView

Bug ID	Description
635309	When FortiAnalyzer logging is configured using an FQDN domain, the GUI displays a 500 error message on the FortiView *Compromised Hosts* page.
673225	FortiView *Top Traffic Shaping* widget does not show data for outbound traffic if the source interface's role is WAN. Data is displayed if the source interface's role is LAN, DMZ, or undefined.

GUI

Bug ID	Description
354464	Antivirus archive logging enabled from the CLI will be disabled by editing the antivirus profile in the GUI, even if no changes are made.
514632	Inconsistent reference count when using ports in HA `session-sync-dev`.
529094	When creating an antispam block/allowlist entry, *Mark as Reject* should be grayed out.
535099	The SSID dialog page does not have support for the new MAC address filter.
541042	Log viewer forwarded traffic does not support multiple filters for one field.
584915	*OK* button missing from many pages when viewed in Chrome on an Android device.
584939	VPN event logs are incorrectly filtered when there are two *Action* filters and one of them contains "-".
602102	Warning message is not displayed when a user configures an interface with a static IP address that is already in use.
602397	Managed FortiSwitch and FortiSwitch *Ports* pages are slow to load when there are many managed FortiSwitches. This performance issue needs a fix on both FortiOS and FortiSwitch. A fix was provided in FortiOS 7.0.1 GA and FortiSwitch 7.0.1 GA.
621254	When creating or editing an IPv4 policy or address group, firewall address searching does not work if there is an empty wildcard address due to a configuration error.
664007	GUI incorrectly displays the warning, *Botnet package update unavailable, AntiVirus subscription not found.*, when the antivirus entitlement is expiring within 30 days. The actual botnet package update still works within the active entitlement duration.
672599	After performing a search on firewall *Addresses*, the matched count over total count displayed for each address type shows an incorrect total count number. The search functionality still works correctly.
682440	On *Firewall Policy* list, the tooltip for *IP Pool* incorrectly shows *Port Block Allocation* as being exhausted if there are expiring PBAs available to be reallocated.
688994	The *Edit Web Filter Profile* page incorrectly shows that a URL filter is configured (even though it is not) if the URL filter entry has the same name as the web filter profile in the CLI.
695163	When there are a lot of historical logs from FortiAnalyzer, the FortiGate GUI *Forward Traffic* log page can take time to load if there is no specific filter for the time range. **Workaround**: provide a specific time range filter, or use the FortiAnalyzer GUI to view the logs.

Intrusion Prevention

Bug ID	Description
565747	IPS engine 5.00027 has signal 11 crash.
586544	IPS intelligent mode not working when reflect sessions are created on different physical interfaces.
587668	IPS engine 5.00035 has signal 11 crash.
590087	When IPS pcap is enabled, traffic is intermittently disrupted after disk I/O reaches IOPS limit.
721462	Memory usage increases up to conserve mode after upgrading IPS engine to 5.00239.

Log & Report

Bug ID	Description
606533	User observes `FGT internal error` while trying to log in or activate FortiGate Cloud from the web UI.

REST API

Bug ID	Description
584631	REST API admin with token unable to configure HA setting (via login session works).
713445	For API user tokens with CORS enabled and set to wildcard *, direct API requests using this token are not processed properly. This issue impacts FortiOS version 5.6.1 and later. **Workaround**: set CORS to an explicit domain.
714075	When CORS is enabled for REST API administrators, POST and PUT requests with body data do not work with CORS due to the pre-flight requests being handled incorrectly. This only impacts newer browser versions that use pre-flight requests.

Routing

Bug ID	Description
537354	BFD/BGP dropping when `outbandwidth` is set on interface.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.

SSL VPN

Bug ID	Description
505986	On IE 11, SSL VPN web portal displays blank page title *{{::data.portal.heading}}* after authentication.

Switch Controller

Bug ID	Description
588584	GUI should add support to allow using switch VLAN interface under a tenant VDOM on a managed switch VDOM.
605864	If the firewall is downgraded from 6.2.3 to 6.2.2, the FortiLink interface loses its CAPWAP setting.

System

Bug ID	Description
464340	EHP drops for units with no NP service module.
578031	FortiManager Cloud cannot be removed once the FortiGate has trouble with contract.
595244	There is duplicate information when checking interface references in global.
600032	SNMP does not provide routing table for non-management VDOM.
607565	Interface `emac-vlan` feature does not work on SoC4 platform.
694202	`stpforward` does not work with LAG interfaces on a transparent VDOM.
724085	Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled. If `auto-asic-offload` is disabled in the firewall policy, then the traffic flows as expected.

Upgrade

Bug ID	Description

658664	FortiExtender status becomes `discovered` after upgrading from 6.0.10 (build 0365).
	Workaround: change the `admin` from `discovered` to `enable` after upgrading.
	`config extender-controller extender`
	`edit <id>`
	`set admin enable`
	`next`
	`end`

User & Device

Bug ID	Description
595583	Device identification via LLDP on an aggregate interface does not work.

VM

Bug ID	Description
587757	FG-VM image unable to be deployed on AWS with additional HDD (st1) disk type.
596742	Azure SDN connector replicates configuration from primary device to secondary device during configuration restore.
605511	FG-VM-GCP reboots a couple of times due to kernel panic.
608881	IPsec VPN tunnel not staying up after failing over with AWS A-P cross-AZ setup.
640436	FortiGate AWS bootstrapped from configuration does not read SAML settings.
668625	During every FortiGuard UTM update, there is high CPU usage because only one vCPU is available.
685782	HTTPS administrative interface responds over heartbeat port on Azure FortiGate despite `allowaccess` settings.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.